DESIGNING OF ALGORITHM FOR ENHANCING NETWORK SECURITY IN MOBILE AD HOC NETWORKS THROUGH INTRUSION DETECTION

A SYNOPSIS

Submitted for the Registration for the Degree

of

Doctor of Philosophy

in the

Computer Application
Faculty of Science

by

Vikas
(Regn. No: SVSU/Ph.D./)
Enrollment Number: 2306000002290

Under the Supervision of

Dr. Shashiraj Teotia

Department of Computer Application
Faculty of Science
Swami Vivekanand Subharti University
(NAAC Accredited grade "A" University)
Subhartipuram, NH-58, MEERUT-25005

(2023-2024)

1. INTRODUCTION

The swift advancement of communication technology and associated services has led to an astonishing level of seeming self-contained communication. The Mobile Ad Hoc Networks (MANETs) illustrate such a set of self-organizing communications that show no systematic structure or fixed foundations. Anywhere mobile devices exist, these networks can spontaneously establish and break temporary connections, facilitating the mobile devices' seamless interaction without a rigid framework. Even through incredible benefits, the profound endorsement of enigmatic mobile networks becomes a double-edged sword. The easy and unshielded availability and open nature of MANET systems makes them particularly vulnerable to endless risks. Each sector that makes use of these networks, be it military within a war zone, healthcare in emergency settings, or use by civilians, amplify the demand for holistic mechanisms aimed at refining their unparalleled threats. Implementing sophisticated intrusion detection systems is critical for the continual protection of MANET networks. The identification of deep structures alongside gaps existing within the domain of security is what this article intends to fill and broaden the scope of mobile networks durability under the new emerging perils of safety. The interconnected nature of advancements in communication such as the evolution of MANETs have transformed a wide array of industries. These self-organizing networks devoid of fixed topology permit mobile devices to communicate by forming dynamic connections. Nevertheless, the features that make MANETs adaptable and flexible are the same features that place them at the risk of security attacks and other forms of malicious exploits. This research sets out to define security with particular regard to the protection of MANETs networks by focusing on the importance of the IDS. The first chapter serves as a window to the complexity of the remaining challenges in MANETs with regard to the secure communication interfaces.

Essentially the purpose of this research is to begin to address the gap towards the tight security arrangement and set level of non-homogeneous architecture and operational behavior of MANETs. This introduction seeks to make preliminary remarks on the complex relations which exist between the features of MANETs and the threats to security they encounter.

Characteristics of MANETs: The decentralized nature of MANETs is their most important feature, where nodes are managed as independent entities that establish ad hoc connections without the aid of any existing infrastructure. This feature enables the on-the-fly formation and reorganization of a network, fundamental to situations such as emergency response, unharnessed military communications, and machine-to-machine interaction in smart environments. Nonetheless, missing a singular authoritative decision-maker yields gaps in security, as networked devices can be hacked or even bring harmful activities to the network.

Security Challenges in MANETs: Automated networks of mobile devices (MANET) are extremely unsecure in comparison to traditional mobile networks hence they come with many

security risks. Security features meant for mobile networks are inadequate in this case. Their resources, node mobility, open medium communication, and missing security perimeters are open to many attacks like eavesdropping, packet dropping, black holes, and even spoofing. The absence of fixed infrastructure intensifies the problem which makes it necessary to develop new ways of safeguarding information systems.

Significance of Intrusion Detection Systems (IDS): Amid these security threats, IDS offer a piece of good news because they work for security gaps in the network. An Intrusion Detection System, which monitors a network for suspicious conduct and issues alerts is precisely what mobile networks require. Through the use of anomaly detection, signature-based detection, or hybrid ways, these systems promise to help in identifying security breaches in mobile networks.

2. LITERATURE SURVEY

Krishnan et al. (2020) discussed a modified zone-based intrusion detection system with respect to security improvements in mobile ad hoc networks. However, there is little or no analysis of the possible difficulties that may come from trying to implement such a system. In addition, the authors provide an analysis of their proposed system, but it is not adequate.

Ponnusamy et al. (2022) reported on the application of IDS in the Internet of Things. The study also focusses and discover the reasons MANets, but there was not a sufficient and coherent presentation of the different systems. On top of that, they didn't explain all of the details of the particular trends and issues pertaining to the solutions they offered.

Bala et al. (2019) created advanced IDS for mobile ad hoc networks using traffic pattern recognition, but the system has not been properly validated. The writers did not argue their system sufficiently.

As noted, the work of Islabudeen and Kavitha Devi (2020) does discuss mobile ad hoc networks, but it is more general in nature. It does not sufficiently explain the security risks and does not explain how the proposed intrusion detection and deterrent system can actually be implemented in the real world. Besides, the authors did not provide any proof of the effectiveness of the claimed system.

Marchang, Datta, and Das (2016) make a bold attempt at mobile networks which are ad hoc in nature to increase the efficiency of invasion uncovering systems. Still, they do not provide an adequate explanation of the new system, which indeed raises doubts regarding its success. Moreover, the authors discuss very few of the available threats to portable ad hoc communication networks.

Sun et al. (2007) provides a survey on techniques of invasion uncovering of mobile ad hoc. wireless sensor networks but offers no information related to safety in these networks. In addition, the article does not bring any novelties with regard to the description of detection of intrusions.

Poongothai and Duraiswamy (2014) came up with an approach for intrusion detection in mobile Ad-Hoc networks that employs ML. While the research gives a holistic summary in this regard, it does not address the possible shortcomings of the technique. In addition, there is no attempt from the authors to validate their approach in practice.

Husain et al. (2010) proposes a system for intrusion detection for ad hoc mobile networks, but does not include any proof for this assertion. Also, the authors do not analyze the adverse effects that might come from executing the proposed model.

Meddeb et al. (2023) offered an approach for attack detection in mobile Ad-hoc networks using Deep Learning. This method, however, does not take into consideration both the volatile nature of these networks as well as what the nodes dynamically do. Furthermore, the author's proposed algorithm does little to resolve these criticisms.

Gupta and Jain (2011) have not provided sufficient proof to support their effort in resolving security issues in the MANETS. Additionally, the authors overlook potential opportunity costs that might result from the hypothesized solution.

Singh et. Al. (2017) describes the intelligent intrusion detection and prevention system for mobile ad hoc networks, but fails to evaluate its effectiveness. Also, the authors fail to adequately address the scalability and performance limitations of the system.

Bouhaddi, Radjef and Adi (2018) describes the comparatively simple intrusion approach for resource-limited mobile ad-hoc networks. However, the authors were unable to present a complete analysis that would show the system's performance in reality. Furthermore, there is little discussion on the anticipated impact of the proposed system on the existing network security infrastructure.

Pamarthi & Narmadha (2022) includes the literature review on the network security of Wireless Mobile Ad-hoc Network (WMAN) for Internet of Things (IoT) applications. However, the authors seem to lack any contemporary attack analysis or evaluation on the network intrusion detection system under consideration.

This work does nothing to address ‘Alnaghes and Gebali’s (2015) article on the survey of intrusion detection systems for mobile networks’ which relied far too much on literature review archetypes and not enough on primary research. Furthermore, no attempt was made to critique the systems cited in the articles.

Sarika et al (2016) offers a rather wide perspective on security issues in MANETs. Still the authors do not provide enough analysis of the security threats, examine existing mechanisms of security, or, what is worse, offer the implementation of particular security mechanisms into the MANETs.

Khanpara and Trivedi (2017) researched the problem of security provision in mobile ad hoc networks, and while they identified these issues sufficiently, their solution was overly complex and lacked directions in terms of practical implementation. There is more to be done on this issue.

Vaseer, Ghai, and Ghai (2019) tried to develop new methodologies for intrusion detection and prevention within a mobile ad hoc network. Their methods evaluation was a bit too cursory for one to grasp the extent of the solutions they offered. In addition, the article failed to be holistic by being based on one single and one multiple attack cases only.

Prasad, Tripathi, S., Dahal K. (2022) suggested a watchguard framework to mitigate attacks in MANet routing, but they did not resolve the issues regarding false positive rates and network intricacy. Their recommendation was focused and did not provide an answer to the overarching issue at hand.

Reddy, Khan, Basha (2019) describes in detail an improved intrusion detection system (IDS) for detection of malignant nodes in mobile ad hoc networks. He did not provide discussion on the shortcomings of the system, which makes his proposal rather ineffective. Also, the article does not specify how the system performs using actual data.

Khalifa et al. (2021) recommended the application of supervised ML as a preventive measure in mobile ad hoc networks. Nonetheless, the proposal was not substantiated with an appropriate evaluation, leaving the effectiveness of the technique unknown. Furthermore, there was no mention of the proposed method's security weaknesses.

Khan et al. (2020) summarizes the issues of wireless ad-hoc networks for monitoring and intrusion prevention, but does not analyze the existing approaches systematically. Also, the paper fails to articulate the discussion of the findings or provide any novelty.

Muruganandam, Srinivasan & Sivaprakasam (2022) came up with new idea for watching over Mobile Ad Hoc networks to protect from threats, but did not describe clearly how the proposal is implemented and what the limitations are. In addition, the authors did not clearly state what the implications of the proposals are.

Albers et al. (2002) Each attempts to deal with the problem of security of the Ad Hoc Networks by proposing General-Intrusion-Detection-Architecture which has trust components. With this, they hope to alleviate some of the security issues. But they do not deal adequately with the

troubles of security in Ad Hoc Network and the “solution” has no constructive details of actual aid towards implementation.

3. SCIENTIFIC GAPS

1. Flexible Character of MANETs: Due to the changing network topology, a feature of MANETs, attempt for intrusion detection systems (IDS) becomes harder. Research could look into designing driven IDS methods which take into account the flexible nature of MANETs.
2. Shortage of Resources: Mobile ad hoc Network (MANET) nodes, or devices, often have processing and energy capabilities. Research could look into resource-frugal intrusion detection systems that would be as accurate as possible while using the least possible resources.
3. Sharing of Information: The collaboration of nodes for the purpose of intrusion detection is one of the areas which needs some study. Look at how nodes can be able to relay information pertaining to possible attacks while at the same time safeguarding their security and privacy.
4. Cost-effective Detection of Intrusion: Since there are little amounts of energy available on the network the detection algorithms must be designed with those restrictions in mind. Monitor experiments that reduce power use while maintaining detection rates.
5. Aggressive Attacks and Their Counter Actions: Come up with new categories of attacks against targeted MANETS and suggest defences. This might include looking into insider attack effects and constructing some form of detection which is immune to hostile paradigms.
6. Anomaly Detection in MANETs: Work may be done on attempting to improve the techniques applied in anomaly detection in mobile networks. This means that there is a requirement to comprehend what the normal behavior of the network is and try to find some inconsistencies which could assist in detecting some abnormal behavior.
7. Defense in Depth in Routing Protocols: Because of the great importance of routing procedures in MANETs, there is a corresponding inadequacy concerning the security of these procedures. Analyze how intrusion detection systems could be utilized in routing processes to identify and respond to attacks focused on the routing system.
8. Preserve Privacy: Attempt to resolve the problem of detection intrusions while also making sure that intrusions individually are made private. Create policies that will enable nodes to disseminate information while concealing their internal states.
9. Policy-based Machine Learning Approaches: Researching how machine learning and artificial intelligence could be utilized for the purpose of intrusion detection for mobile ad hoc networks. Including forming algorithms that would address the adaptive nature of networks and the new challenges that come with them.

10. Real World Deployments and Testing: Too many attempts of intrusion detection are lacking practical attempts of verification. Their focus could be on the restrictions and constraints of particular operational conditions and study how those conditions affect the functioning of intrusion detection systems in MANETs.

4. OBJECTIVES

Research Aims & Objectives:

Mobile Ad Hoc Networks (MANETs) offer a new and sophisticated form of communication technology that allows for self-organizing and transient connectivity. Nonetheless, their exposure to security threats calls for new approaches to protect the information exchange. In this part, I explain the overarching aims and objectives of the research, presenting a strategy to close identified gaps and enhance the security of MANETs with an Intrusion Detection System (IDS).

Research Aim:

This dissertation attempts to enhance the theory and practice of securing Mobile Ad Hoc Networks (MANETs) using an Intrusion Detection System (IDS) algorithm via systems theoretic methodologies. Its aim is to construct a comprehensive framework that integrates both the theoretical and practical components of security within the context of MANETs.

Objectives:

1. **To Evaluate Existing Security Mechanisms in MANETs**
2. **To Identify and characterize MANET-Specific Security Threats**
3. **To Develop an adaptive Intrusion Detection System [IDS]**
4. **To Evaluate and Validate the IDS in Real-World MANET Scenarios**

5. METHODOLOGY

Kind of Research/Design: This research adopts a blended approach, utilizing both methods and materials of qualitative and quantitative research. This approach allows a comprehensive exploration of the intricacies associated with enhancing network security in Mobile Ad Hoc Networks (MANETs) with an Intrusion Detection System (IDS) technology.

Population: The population covers a wide scope of a MANET which includes both artificial and real-world systems. This variation ensures that the developed Intrusion Detection System will be functional and effective in a large number of operating networks.

Sample/Sampling Design: There is a purposeful selection of sample design to select the subset of scenarios that correspond to the boundaries of the MANET to be studied. This design enhances the chances of capturing diverse network topologies and mobility patterns and application contexts for evaluating the proposed IDS to the greatest extent possible.

Setting: The study is carried out in simulations and actual settings. The simulations enable an accurate assessment of the Intrusion Detection System's performance and effectiveness, whereas the actual settings include military exercises, disaster response simulations, and smart city deployments, which provide insights into the practical usefulness and adaptability of the system.

Method: The research methodology includes the following main elements.

Intervention & Duration: The proposed Intrusion Detection System is designed, implemented, and tested as an intervention. The intervention occurs over a specified period which encompasses system design, simulation, deployment, and performance evaluation. The timeline is set to account for the difficulties encountered in the design and validation of an adaptive IDS for MANETs.

Data Gathering: Data collection adopts an eclectic approach :

• **Network Traffic Study:** Collect network traffic data from both simulated and actual MANETs to analyze communication patterns, find irregularities, and create intrusion simulations.

• **Simulation of Intrusion Scenarios:** Create and implement multiple intrusion scenarios for an evaluation of an IDS's detection and response capabilities against differing forms of security threats.

• **Evaluation of Performance Metrics:** Measure and record results pertaining to various performance metrics such as detection accuracy, false positive rate, response time, and other quantitative values in order to assess the proposed IDS objectively.

Evaluation Tools: The research incorporates a mix of evaluation tools:

• **Algorithms of Intrusion Detection:** Design and apply the algorithms of intrusion detection of systems with anomaly detection combined with signature-based detection and/or hybrid methods of the specific context of the MANET.

• **Tools of Measurement of Performance:** Apply the tools for assessment of the operation of the IDS such as open-source network simulators, intrusion detection evaluation frameworks, and statistical software.

Likely Future Outcomes: The respectively envisions multiple prospective outcomes as follows:

• **Verification of Expected IDS:** Achieving verification of the expected IDS, which ascertains the existence of security breaches and the reduction of risks attributed to threats in MANETs.

• **Determination of Ideal Parameters:** Determination of ideal parameters and other relevant system design specifications for the IDS given the network features, thus offering useful guidance for implementation.

• **Addition to Existing Body of Knowledge in MANET Security:** Add increase in the scholarly and practical debate in the field of MANET security by providing an understanding on the gaps within the already established security systems and directions for other studies.

Essentially, the methodology of the research is aimed at comprehensively examining and validating the proposed IDS, particularly its functionality in different MANET environments, and in turn, advance the field of network security.

6. BIBLIOGRAPHY / REFERENCES

1. Krishnan, R. S., Julie, E. G., Robinson, Y. H., Kumar, R., Son, L. H., Tuan, T. A., & Long, H. V. (2020). Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks. Wireless Networks, 26, 1275-1289.
2. Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Yichiet, A., & Almufareh, M. F. (2022). Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks. Computer Systems Science & Engineering, 40(3).
3. Bala, K., Jothi, S., & Chandrasekar, A. (2019). An enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis. Cluster Computing, 22, 15205-15212.
4. Islabudeen, M., & Kavitha Devi, M. K. (2020). A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks. Wireless Personal Communications, 112, 193-224.
5. Marchang, N., Datta, R., & Das, S. K. (2016). A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks. IEEE Transactions on Vehicular Technology, 66(2), 1684-1695.
6. Sun, B., Osborne, L., Xiao, Y., & Guizani, S. (2007). Intrusion detection techniques in mobile ad hoc and wireless sensor networks. IEEE Wireless Communications, 14(5), 56-63.

7. Poongothai, T., & Duraiswamy, K. (2014, February). Intrusion detection in mobile AdHoc networks using machine learning approach. In International Conference on Information Communication and Embedded Systems (ICICES2014) (pp. 1-5). IEEE.
8. Husain, S., Gupta, S. C., Chand, M., & Mandoria, H. L. (2010, September). A proposed model for Intrusion Detection System for mobile adhoc network. In 2010 International Conference on Computer and Communication Technology (ICCCT) (pp. 99-102). IEEE.
9. Meddeb, R., Jemili, F., Triki, B., & Korbaa, O. (2023). A deep learning-based intrusion detection approach for mobile Ad-hoc network. Soft Computing, 1-15.
10. Gupta, R., & Jain, C. (2011). Mobile Ad hoc Network (MANETS): Proposed solution to Security Related Issues. Indian journal of computer science and Engineering (IJCSE), 2(5), 738-746.
11. Singh, O., Singh, J., & Singh, R. (2017). An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes. Indian Journal of Science and Technology, 8(1), 1-12.
12. Bouhaddi, M., Radjef, M. S., & Adi, K. (2018). An efficient intrusion detection in resource-constrained mobile ad-hoc networks. Computers & Security, 76, 156-177.
13. Pamarthi, S., & Narmadha, R. (2022). Literature review on network security in Wireless Mobile Ad-hoc Network for IoT applications: network attacks and detection mechanisms. International Journal of Intelligent Unmanned Systems, 10(4), 482-506.
14. Alnaghes, M. S., & Gebali, F. (2015, May). A survey on some currently existing intrusion detection systems for mobile ad hoc networks. In The Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing (EEECEGC2015) (Vol. 12).
15. Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security issues in mobile ad hoc networks. Procedia Computer Science, 92, 329-335.
16. Khanpara, P., & Trivedi, B. (2017). Security in mobile ad hoc networks. In Proceedings of International Conference on Communication and Networks: ComNet 2016 (pp. 501-511). Springer Singapore.
17. Vaseer, G., Ghai, G., & Ghai, D. (2019). Novel intrusion detection and prevention for mobile ad hoc networks: A single-and multiattack case study. IEEE Consumer Electronics Magazine, 8(3), 35-39.
18. Prasad, M., Tripathi, S., & Dahal, K. (2022). An enhanced detection system against routing attacks in mobile ad-hoc network. Wireless Networks, 28(4), 1411-1428.
19. Reddy, B. P., Khan, P. I., & Basha, S. M. (2019). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 10(3), 1439-1444.
20. Khalifa, M. M., Ucan, O. N., & Alheeti, K. M. A. (2021, December). Supervised Machine Learning to Enhance Security in Mobile Ad Hoc Networks. In 2021 14th International Conference on Developments in eSystems Engineering (DeSE) (pp. 493-498). IEEE.

21. Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K. (2020). A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture, 105, 101701.
22. Alamdarloo, A. N., Mirabedini, S. J., & Abadi, A. H. (2016). A Secure Method Intrusion Detection System for Routing Attacks in Mobile Ad-Hoc Networks. International Journal of Computer Science and Information Security, 14(8), 1019.